Information Commissioner's Office

Internal Audit 2013-14: Risk Management and Horizon Scanning

Last updated 24 June 2014

Distribution		Timetable	
For action	Director of Corporate Services	Fieldwork completed	6 May 2014
For information	Senior Corporate Governance Manager	Draft report issued	8 May 2014
For information	Audit Committee	Management comments	20 May 2014
		Final report issued	21 May 2014

It is the responsibility solely of the ICO management to ensure that there are adequate arrangements in place in relation to risk management, governance and control.

1 Executive Summary

1.1 Background

The ICO Plan 2013-2016 states that the ICO "face a series of policy challenges that will put the ICO even more at the centre of events, even if the precise terms of the ICO's involvement are less than clear. We need to assess their impact and the implications for the ICO." The report also asserts that "In the light of these challenges, the ICO is taking a long hard look at itself to discern the way forward, reviewing the different scenarios and options."

Risk management and the identification of emerging risks is central to the ICO's ability to deal effectively with such a challenging landscape.

1.2 Scope

Our review involved an assessment of the following risks:

- The ICO may not have appropriate mechanisms/platforms to identify and monitor emerging risks/challenges/uncertainties, resulting in an inability for the organisation to identify how it will respond to such risks etc. and potentially being adversely impacted should the risk crystallise; and
- There may be a disconnect between the organisation's risk management and corporate planning arrangements, resulting in objectives and strategies being pursued that do not fully identify the risks associated with them.

Further details on responsibilities, approach and scope are included in Appendix A.

1.3 Overall assessment

We have made an overall assessment of our findings as:

Overall assessment	
We have identified matters which, if resolved, will help management fulfil their responsibility to maintain a robust system of internal control.	Green

Please refer to appendix B for further information regarding our overall assessment and audit finding ratings.

1.4 Key findings

Risk / Process	High	Medium	Low	Imp
Platforms for identifying and monitoring risks	-	-	-	2
Connection between risk and corporate planning processes	-	1	-	-
Total	**-**	**1**	**-**	**2**

The following finding was rated as medium priority:

- There is a disconnect between the Corporate Risk Register and the risks associated with achieving the 2014-17 Plan. Neither the Corporate Risk Register nor the ICO Plan identify the risks associated with delivering the Plan.

Further details of our findings and recommendations are provided in Section 2.

1.5 Basis of preparation

Whilst we report by exception, we draw attention to the following matters in addition to the issues raised within the findings section of this report.

- Risks and the issues the drive the risks are regularly reviewed through Executive Team, Information Rights Committee, Management Board and the Audit Committee as part of the governance cycle. The Information Commissioner's updates to Management Board and Audit Committee in particular are seen as one of the tools through which current and future challenges, often external to the organisation, are highlighted and discussed, by both Executive and Non-Executive staff.
- All whom we met with held the view that risks to the organisation are identified across the organisation and discussed at the forums identified above.
- Due to much of the ICO's work being driven by Government policy, it has to be reactive to situations that arise, however its communication channels with the Ministry of Justice help the ICO engage at different levels to make clear the impact of policy issues on the operations of the ICO. There is an awareness that whilst the ICO is aware of future challenges, due to the size of the organisation it is difficult for the ICO to always identify how best it can respond.

1.6 Elsewhere in the sector

We detail below other ways of working and commonly occurring issues that we have experienced during similar types of reviews for other public bodies. The following does not necessarily purport to be good practice but is included for your information and consideration.

- An organisation we work with has internal business planning documents that underpin its public facing strategic plan. These documents identify the activities being carried out to deliver the strategic plan, success measures and associated risks across its key areas of activity. These are used to formulate its corporate risk register, in the process hard-wiring the risks associated with delivering its strategic plan.
- Many of the not-for-profit/public sector organisations we work with are having to focus on how they need to operate in order to discharge their responsibilities but with fewer resources. To achieve this, we are seeing:
  - Senior management taking more time to understand the opportunities and associated risks that they could/need to take in order to operate differently, or for less.
  - Boards scrutinising financial plans and models that identify different ways of working.
  - Different aspects of the organisations are having to work more collaboratively to identify the threats and opportunities that they face.
  - Strategies developed that not only set out how the mission and values will be achieved, but also how the infrastructure of the organisation will change to achieve it.

1.7 Acknowledgement

We would like to take this opportunity to thank the staff involved for their co-operation during this internal audit.

2 Detailed Findings

2.1 Connection between risk and corporate planning processes

1.	Medium	Alignment between ICO Plan 2014-17 and the associated risks

Finding and Implication	Proposed action	Agreed action *(Date / Ownership)*
Whilst we acknowledge that the future challenges and drivers behind the ICO Plan 2014-17 and the risks that the organisation faces are understood and discussed regularly, there is a disconnect between the Corporate Risk Register and the risks associated with achieving the 2014-17 Plan. This reflects previous analysis that showed that most risks fell under just one of the ICO's six aims. The ICO's Risk Management Policy does define risk as something that will stop the ICO achieving its aims, However neither the Corporate Risk Register nor the ICO Plan explicitly identifies the risks associated with delivering the Plan. We understand the purpose of the ICO Plan as a public facing stakeholder engagement document, and that it would not be appropriate to identify the risks to its achievement within it. However, the Corporate Risk Register could be used to capture these risks that fall outside of those already identified, as either strategic risks or long term risks associated with delivering strategic objectives.	Expand the Corporate Risk Register to capture those risks associated with delivering the ICO Plan.	*Agreed action:* *Exercises be regularly (at least annually) undertaken with Executive Team and Leadership Group (as appropriate) to explicitly consider risks against the ICO achieving each of its six aims detailed in the ICO Plan.* *The results of the exercises to be incorporated within the Risk Register.* *Date Effective:* *31 August 2014* *Owner:* *Daniel Benjamin*

2.2 Platforms for identifying and monitoring risks

2.	Improvement	Capturing emerging risks

Finding and Implication	Proposed action	Agreed action *(Date / Ownership)*
Management recognises that the ICO faces challenges and uncertainty (e.g. the implications on its operations of changing EU legislation) that are mainly outside its control . While these are raised and discussed through a variety of fora within the organisation, they are not captured on the Corporate Risk Register. We appreciate that it may not be possible to populate the risk template for these risks due to levels of uncertainty as to their impact, however by capturing them as emerging risks will formalise their existence and enable them to be reviewed and discussed by Executive Team, the Audit Committee and the Management Board as part of the risk management framework.	The Corporate Risk Register to be used to document emerging risks and challenges that the ICO sees itself facing.	*Agreed action:* *We are already experimenting; using a timeline to identify known and possible issues that are coming up; eg the general election and end of the lease, to help identify possible risks associated with these issues.* *The risk register will also include a list of emerging risks and challenges as they are identified in whatever fora.* *Date Effective:* *July Management Board (28 July 2014)* *Owner:* *Daniel Benjamin*

2.3 Platforms for identifying and monitoring risks

3.	Improvement	Risk analysis

Finding and Implication	Proposed action	Agreed action *(Date / Ownership)*
Organisations we work with are developing a coordinated focus on risk identification within the environment within which they operate. As part of this, management teams are working together to more regularly identify the risks and opportunities that they face. Whilst we are aware that discussions of this nature take place at the Executive Team, there is an opportunity for the Leadership Group to play an active role in formally identifying the risks and opportunities that the ICO faces in both the long and short term to help provide focus for the Executive Team and Management Board in it is discussions.	The Leadership Group to carry out reviews of the risks and opportunities that the ICO faces, potentially using SWOT or PESTLE as a framework for analysis. This could also be a forum where emerging risks are discussed and reflected upon against the Corporate Risk Register and ICO Plan.	*Agreed action:* *The response to action 1 includes Leadership Group as a forum for looking at risks. The exercise would be built around relevant techniques and would include identification of emerging as well as existing risks.* *Date Effective:* *31 August 2014* *Owner:* *Daniel Benjamin*

A Internal audit approach

Approach

Our role as internal auditor to a Public Body is to provide an independent and objective opinion to the Accounting Officer on risk management, control and governance processes, by measuring and evaluating their effectiveness in achieving the organisation's agreed strategic objectives.

Our audit was carried out in accordance with the guidance contained within the Government's Internal Audit Standards (2013) and the Auditing Practices Board's 'Guidance for Internal Auditors'. We also had regard to the Institute of Internal Auditors' guidance on risk based internal auditing (2005). In addition, we comply in all material respects with other Government guidance applicable to Public Bodies and have had regard to the HM Treasury guidelines on effective risk management (the 'Orange Book').

Our aim in completing this audit was to ensure that the ICO has appropriate arrangements in place to identify, manage and report on risk.

We achieved our audit objectives by:

- Identifying and challenging where in the organisation potential new risks, challenges or uncertainties are identified and the routes through which they are communicated;
- Assess the consideration of risks as part of the preparation of the corporate plan; and
- Comparing ICO practices to other organisations and clients we work with as appropriate to provide relevant insight.

The findings and conclusions from this review will support our annual opinion to the Audit Committee on the adequacy and effectiveness of risk management arrangements.

Responsibilities

The Information Commissioner acts through his Board of Management and the Information Commissioner's Office ("ICO") discharges his obligations. Therefore references to the Information Commissioner and the ICO in this report relate to one and the same party.

It is the responsibility of the Information Commissioner to ensure that the ICO has adequate and effective risk management, control and governance processes.

HM Treasury's Corporate Governance in Central Government Departments (2011) states that boards of Public Bodies should determine the nature and extent of the significant risks it is willing to take in achieving its strategic objectives. The Board should therefore maintain sound risk management and internal control systems and should establish formal and transparent arrangements for considering how they should apply the corporate reporting and risk management and internal control principles and for maintaining an appropriate relationship with the organisation's auditors.

Please refer to our letter of engagement for full details of responsibilities and other terms and conditions.

B Overall assessment and audit issues ratings

Overall assessment

Rating	Description
Red	Following agreement of the nature and significance of individual issues with management, in our view this report contains matters which should be raised with Senior Management and the Audit Committee at the earliest opportunity.
Amber	Following agreement of the nature and significance of individual issues with management, in our view this report contains matters which require the attention of management to resolve and report on progress in line with current follow up processes.
Green	We have identified matters which, if resolved, will help management fulfil their responsibility to maintain a robust system of internal control.

Audit issue rating

Within each report, every audit issue is given a rating. This is summarised in the table below.

Rating	Description	Features
High	Findings that are fundamental to the management of risk in the business area, representing a weakness in control that requires the immediate attention of management	• Key control not designed or operating effectively • Potential for fraud identified • Non-compliance with key procedures / standards • Non-compliance with regulation
Medium	Important findings that are to be resolved by line management.	• Impact is contained within the department and compensating controls would detect errors • Possibility for fraud exists • Control failures identified but not in key controls • Non-compliance with procedures / standards (but not resulting in key control failure)
Low	Findings that identify non-compliance with established procedures.	• Minor control weakness • Minor non- compliance with procedures / standards
Improvement	Items requiring no action but which may be of interest to management or best practice advice	• Information for department management • Control operating but not necessarily in accordance with best practice

"Grant Thornton" refers to the brand under which the Grant Thornton member firms provide assurance, tax and advisory services to their clients and/or refers to one or more member firms, as the context requires.

Grant Thornton UK LLP is a member firm of Grant Thornton International Ltd (GTIL). GTIL and the member firms are not a worldwide partnership. GTIL and each member firm is a separate legal entity. Services are delivered by the member firms. GTIL does not provide services to clients. GTIL and its member firms are not agents of, and do not obligate, one another and are not liable for one another's acts or omissions.

grant-thornton.co.uk